What is claimed is:

1. A rights management method comprising:

(a) receiving an information signal;

(b) steganographically decoding the received information signal to recover digital rights management control information; and

(c) performing at least one rights management operation based at least in part on the recovered digital rights management control information.

2. A method as in claim 1 wherein receiving step (a) comprises receiving an analog signal steganographically encoded with the digital rights management control information, and decoding step (b) comprises steganographically decoding the analog signal.

3. A method as in claim 1 wherein performing step (c) comprises the step of selectively enabling descrambling of the information signal.

4. A method as in claim 1 wherein performing step (c) comprises the step of selectively enabling decrypting of the information signal.

5. A method as in claim 1 wherein decoding step (b) comprises recovering digital rights management control information

packaged within at least one digital container, and performing step (c) comprises performing the rights management operation based at least in part on the recovered digital rights management control information.

6. A method as in claim 1 wherein the decoding step (b) includes the step of steganographically decoding information representing at least one permissions record.

7. A method as in claim 1 further including the step of decrypting contents of the digital container for use in performing step (c).

8. A method as in claim 1 wherein the information signal carries further information in addition to the steganographically encoded information, and the performing step (b) comprises the step of managing at least one right in respect of the further information.

9. A method as in claim 1 wherein the decoding step (b) includes the step of analyzing the information signal using a spectral transform.

10. A method as in claim 1 wherein the decoding step (b) includes the step of analyzing the information signal using a key-based steganographic decoder.

11. A method as in claim 1 wherein the decoding step (b) includes the step of steganographically decoding a pointer that points to another portion of the information signal.

12. A method as in claim 1 wherein the steganographically encoded container includes at least one organization structure, and the decoding step (b) comprises steganographically decoding the organizational structure.

13. A rights management method comprising:

(a) receiving an information signal;

(b) steganographically decoding the received information signal to recover at least one rights management permission; and

(c) performing at least one rights management operation based at least in part on the recovered rights management permission.

14. A virtual distribution environment comprising:

plural tamper-resistant protected processing environments coupled together via at least one communications path; and

means for delivering, to the plural tamper-resistant protected processing environments, an information signal having at least one digital rights management control set

substantially invisibly and substantially indelibly encoded thereon.

15. An electronic appliance comprising:

decoding means for steganographically decoding a signal to provide control information; and

rights management means coupled to the decoding means for performing at least one rights management operation based at least in part on the control information.

16. An appliance as in claim 15 wherein the rights management means includes means for means for selectively blocking the signal.

17. An appliance as in claim 15 wherein the rights management means includes means for selectively descrambling the signal.

18. An appliance as in claim 15 wherein the rights management means includes means for authenticating a further appliance before delivering the signal to said further appliance.

19. An appliance as in claim 15 wherein the rights management means includes means for requiring that a further appliance present an appropriate digital certificate before delivering the signal to said further appliance.

20. An appliance as in claim 15 wherein the right management means includes means for fingerprinting the signal based at least in part on the control information.

21. An appliance as in claim 15 wherein the right management means includes means for further steganographically encoding the signal based at least in part on the control information.

22. An electronic appliance comprising:

a steganographic decoder that steganographically decode a signal to provide control information; and

rights management component coupled to the decoder, the rights management component performing at least one rights management operation based at least in part on the control information.

23. An appliance as in claim 22 wherein the rights management component includes or controls a signal blocking circuit that selectively blocks the signal.

24. An appliance as in claim 22 wherein the rights management component includes or controls a signal descrambler.

25. An appliance as in claim 22 wherein the rights management component includes an authenticating circuit for

authenticating a further appliance before delivering the signal to said further appliance.

26. An appliance as in claim 22 wherein the rights management component includes a circuit for requiring that a further appliance present an appropriate digital certificate before delivering the signal to said further appliance.

27. An appliance as in claim 22 wherein the rights management component includes a circuit for fingerprinting the signal based at least in part on the control information.

28. An appliance as in claim 22 wherein the rights management component includes a circuit for further steganographically encoding the signal based at least in part on the control information.

29. A method of steganographically encoding a signal comprising:

providing at least one organization structure including control information;

selectively encrypting at least a part of the organizational structure;

frequency transforming an input signal;

encoding the input signal with the selectively encrypted organizational structure in such a way so as to make the

encoded organizational structure substantially indelible and substantially invisible; and

delivering the encoded input signal.